

## XOOPS Security Advisory - XOOPS

NEWS\_PDF\_AUTHOR: Boobtoob

NEWS\_PDF\_DATE: 2002/12/19 22:08:38

**A security vulnerability within the Visitors 2 module has been brought to our attention.**

The XOOPS team would ask that anyone using this module, please discontinue it's usage by deactivating it and removing the Vistors 2 module from your system completely. The vulnerability makes it possible for someone without any privileges to execute rouge php code on the host system compromising security. As an example, we were handed a sample of our etc/passwd file.

We apologize for any inconvenience this might cause but we strongly advise discontinuing using this module. Since this is not an official XOOPS module, it has been depreciated for the upcoming XOOPS 2 release.

Thanks,  
XOOPS Team

Note: This vulnerability is not possible if allow\_url\_fopen is set to 0 (the default is 1) in the php.ini file.

A security vulnerability within the Visitors 2 module has been brought to our attention.

The XOOPS team would ask that anyone using this module, please discontinue it's usage by deactivating it and removing the Vistors 2 module from your system completely. The vulnerability makes it possible for someone without any privileges to execute rouge php code on the host system compromising security. As an example, we were handed a sample of our etc/passwd file.

We apologize for any inconvenience this might cause but we strongly advise discontinuing using this module. Since this is not an official XOOPS module, it has been depreciated for the upcoming XOOPS 2 release.

Thanks,  
XOOPS Team

Note: This vulnerability is not possible if allow\_url\_fopen is set to 0 (the default is 1) in the php.ini file.